Abstract

A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network. The method comprises negotiating one or more Security Associations between the mobile host and a correspondent host of a Virtual Private Network . Subsequently, a communication is initiated between the mobile host and a Security Gateway and an authentication certificate sent to the Security Gateway, the certificate containing at least the identity of a Security Association which will be used for subsequent communication between the mobile host and the correspondent host. Data packets can then be sent from the mobile host to the correspondent host using the identified Security Association, via the Security Gateway. However, the data packets are forwarded by the Security Gateway to the correspondent host only if they are authenticated by the Security Gateway.